

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (ORIGINAL) A security method of a network accessible apparatus, the security method comprising:
 - identifying whether a command is a reliable request or an unreliable request, wherein a context issues the command to read a content;
 - reading the content and generating a reliable context corresponding to the content when the command is the reliable request; and
 - reading the content and generating an unreliable context corresponding to the content when the command is the unreliable request.
2. (ORIGINAL) The security method of claim 1, further comprising:
 - identifying a reliability of the context based on a flag of a memory into which the context that issues the command is loaded.
3. (ORIGINAL) A security method of a network accessible apparatus, the security method comprising:
 - identifying whether a context is a reliable context or an unreliable context, wherein the context issues a command to perform a specific operation;
 - determining that the specific operation is not permitted when the context is an unreliable context; and
 - not performing the specific operation and outputting an error message when the specific operation is not permitted.
4. (ORIGINAL) The security method of claim 3, wherein the issuing of the command comprises identifying a reliability of the context based on a flag of a memory into which the context that issues the command is loaded.

5. (ORIGINAL) The security method of claim 3, further comprising:
not performing a preload when the context commands to preload a markup document to secure seamless reproduction of AV data and outputting the error message.
6. (ORIGINAL) The security method of claim 3, further comprising:
not performing a deletion when the context commands to delete data that is preloaded in a memory of the network accessible apparatus and outputting the error message.
7. (ORIGINAL) The security method of claim 3, further comprising:
not performing access when the context commands to access data that is recorded on a disk mounted in the network accessible apparatus and outputting the error message.
8. (ORIGINAL) The security method of claim 3, further comprising:
not performing access when the context commands to access another frame through a frame and outputting the error message.
9. (ORIGINAL) The security method of claim 3, further comprising:
not performing access when the context commands to access cookies that are stored in the network accessible apparatus by another context and outputting the error message.
10. (ORIGINAL) The security method of claim 3, further comprising:
not performing access when the context commands to access another context that is operated in the network accessible apparatus and outputting the error message.
11. (ORIGINAL) The security method of claim 3, further comprising:
not performing control when the context commands to control a reproducing engine, which reproduces AV data recorded on a disk mounted in the network accessible apparatus and outputting the error message.
12. (ORIGINAL) A security method of a network accessible apparatus, the security method comprising:
issuing a command by a reliable context to read a content;
identifying whether the command is a reliable request or an unreliable request based on

syntax of the command; and

generating a reliable context corresponding to the content when the command is the reliable request; and

generating an unreliable context when the command is the unreliable request.

13. (ORIGINAL) The security method of claim 12, wherein the content corresponding to the reliable context is recorded on a disk mounted in the network accessible apparatus.

14. (ORIGINAL) The security method of claim 13, wherein the command recorded as an "http://" request in the content corresponding to the reliable context is determined as the reliable request, and the command recorded as an "httpu://" request in the content corresponding to the reliable context is determined as the unreliable request.

15. (ORIGINAL) An information storage medium that is reproducible by a network accessible apparatus, the information storage medium, comprising:
an application content storing command information, wherein the command information is interpreted as a reliable request or an unreliable request.

16. (ORIGINAL) The information storage medium of claim 15, wherein the command information is recorded using syntax to identify whether the command is a reliable request or an unreliable request.

17. (ORIGINAL) The information storage medium of claim 16, wherein the reliable request is recorded as an "http://" request and the unreliable request is recorded as an "httpu://" request.

18. (ORIGINAL) The information storage medium of claim 17, wherein the "http://" request is a command to read a reliable content from the network.

19. (ORIGINAL) The information storage medium of claim 17, wherein the "httpu://" request is a command to read an unreliable content from the network.

20. (ORIGINAL) A network accessible apparatus, comprising:
a reader reading a first content from a disk mounted in the apparatus; and

a presentation engine reading a second content from a network,
wherein the presentation engine generates a first reliable context corresponding to the first content from the disk, and interprets and executes the second content from the network to generate a second reliable context, or interprets and executes the second content from the network to generate an unreliable context.

21. (ORIGINAL) The apparatus of claim 20, wherein the presentation engine identifies the reliability of a context that issues a command to read the second content from the network, to generate the unreliable context corresponding to the second content when the context that issues the command is the unreliable context, and to identify whether the command is a reliable request or an unreliable request when the context that issues the command is a reliable context, to generate the reliable context corresponding to the second content when the command is the reliable request, and to generate an unreliable context corresponding to the second content when the command is the unreliable request.

22. (ORIGINAL) The apparatus of claim 20, wherein the presentation engine examines flags, corresponding to context loaded into a memory to identify whether the context, which has issued the command to read the predetermined content, is the reliable context or the unreliable context.

23. (ORIGINAL) The apparatus of claim 20, wherein the presentation engine examines syntax recorded in the corresponding content to identify whether a command from the first reliable context is a reliable request or an unreliable request.

24. (ORIGINAL) A network accessible apparatus, comprising:
a reader reading a first content from a disk mounted in the apparatus; and
a presentation engine reading a second content from a network,
wherein the presentation engine generates a first reliable context corresponding to the content from the disk, and interprets and executes the second content from the network, which is reliably requested by the first reliable context, to generate a second reliable context, and interprets and executes the second content from the network, which is unreliably requested by the first reliable context to generate an unreliable context, and when a command to perform an operation from the unreliable context is not permitted, the presentation engine does not perform

the operation and outputs an error message.

25. (ORIGINAL) The apparatus of claim 24, wherein when a command to preload a markup document to secure seamless reproduction of AV data is received from the unreliable context, the presentation engine does not perform the preload and outputs the error message.

26. (ORIGINAL) The apparatus of claim 24, wherein when a command to delete data that is preloaded in a memory of the apparatus is received from the unreliable context, the presentation engine does not perform the deletion and outputs the error message.

27. (ORIGINAL) The apparatus of claim 24, wherein when a command to access data that is recorded on the disk mounted in the apparatus is received from the unreliable context, the presentation engine does not perform the access and outputs the error message.

28. (ORIGINAL) The apparatus of claim 24, wherein when a command to access another frame through a frame is received from the unreliable context, the presentation engine does not perform the access and outputs the error message.

29. (ORIGINAL) The apparatus of claim 24, wherein when a command to access cookies that are stored in the apparatus by another context is received from the unreliable context, the presentation engine does not perform the access and outputs the error message.

30. (ORIGINAL) The apparatus of claim 24, wherein when a command to access another context that is operated in the apparatus is received from the unreliable context, the presentation engine does not perform the access and outputs the error message.

31. (ORIGINAL) The apparatus of claim 24, wherein when the command to control the reproducing engine, which reproduces AV data recorded on the disk mounted in the apparatus is received from the unreliable context, the presentation engine does not perform the control and outputs the error message.

32. (ORIGINAL) A network accessible apparatus, comprising:
a reader reading a first content from a disk mounted in the apparatus; and

a presentation engine reading a second content from a network,
wherein the presentation engine identifies a reliability of a command to retrieve the first content, which is received from a reliable context generated from the first content read through the reader, based on a syntax of the command, and
the presentation engine retrieves the second content from the network and generates a reliable context corresponding to the second content in response to the reliable request, and the presentation engine retrieves the second content from the network and generates an unreliable context corresponding to the second content in response to the unreliable request.

33. (ORIGINAL) The apparatus of claim 32, wherein the presentation engine identifies an "http://" request as a reliable request and an "httpu://" request as an unreliable request.

34. (ORIGINAL) The apparatus of claim 32, wherein the content is at least one of a Java program, a script program, and a markup document that is interpreted and executed by the apparatus.

35. (ORIGINAL) The apparatus of claim 24, wherein the network accessible apparatus performs restricted commands from the unreliable contexts to separate the reliable context from the unreliable contexts.

36. (ORIGINAL) The apparatus of claim 25, wherein when producing a content server as the markup documents, the content server is accessible by link tags and the network accessible apparatus determines server reliability.

37. (ORIGINAL) The apparatus of claim 24, wherein the unreliable context cannot generate reliable contexts.

38. (ORIGINAL) The apparatus of claim 32, wherein the unreliable context cannot perform cache control operations.

39. (ORIGINAL) The apparatus of claim 38, wherein when the unreliable context is one frame in a structure having frames, the unreliable context cannot access another frame.

40. (ORIGINAL) The apparatus of claim 39, wherein the unreliable context cannot access cookies that are stored in the reproducing apparatus 1 by another context.

41. (ORIGINAL) The apparatus of claim 40, wherein the unreliable context cannot exchange data with another context.

42. (ORIGINAL) The apparatus of claim 32, wherein the network accessible apparatus performs restricted commands from the unreliable contexts to separate the reliable context from the unreliable contexts.

43. (ORIGINAL) The apparatus of claim 34, wherein when producing a content server as the markup documents, the content server is accessible by link tags and a server reliability is determined by the network accessible apparatus.

44. (ORIGINAL) The apparatus of claim 32, wherein the unreliable context cannot generate reliable contexts.

45. (ORIGINAL) The apparatus of claim 44, wherein the unreliable context cannot perform cache control operations.

46. (ORIGINAL) The apparatus of claim 45, wherein when the unreliable context is one frame in a structure having frames, the unreliable context cannot access another frame.

47. (ORIGINAL) The apparatus of claim 46, wherein the unreliable context cannot access cookies that are stored in the apparatus by another context.

48. (ORIGINAL) The apparatus of claim 47, wherein the unreliable context cannot exchange data with another context.